

CLAIMS

What is claimed is:

- 1 1. A method of preventing an attack on a network, the method comprising the computer-implemented steps of:
 - 3 receiving an ICMP packet that includes a copy of a header associated with a
 - 4 connection in a connection-oriented transport protocol;
 - 5 obtaining a packet sequence value from the header;
 - 6 determining if the packet sequence value is valid;
 - 7 updating a parameter value associated with the transport protocol connection only if
 - 8 the packet sequence value is determined to be valid.
- 1 2. A method as recited in Claim 1, wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that includes a copy of a TCP header associated with a
- 2 TCP connection.
- 1 3. A method as recited in Claim 1, wherein the step of receiving an ICMP packet comprises receiving an ICMP “endpoint unreachable” error packet.
- 1 4. A method as recited in Claim 1, wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that specifies that fragmentation is needed.
- 1 5. A method as recited in Claim 1, wherein the step of determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of packet sequence values that are allowed by the transport protocol for the connection.
- 1 6. A method as recited in Claim 1, wherein the step of determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of sent but unacknowledged TCP packet sequence values for the connection.

1 7. A method as recited in Claim 1, wherein the step of determining if the packet
2 sequence value is valid comprises determining if the packet sequence value is exactly equal
3 to one or more sequence values of one or more packets that are then-currently stored in a
4 TCP re-transmission buffer, starting at a sequence value of a previously sent segment that
5 resulted in receiving the ICMP packet.

1 8. A method as recited in Claim 1, wherein the steps are performed in a router acting as
2 a TCP endpoint node.

1 9. A method as recited in Claim 1, wherein the steps are performed in a firewall device.

1 10. A method of preventing an attack on a network, the method comprising the computer-
2 implemented steps of:

3 receiving, at a TCP endpoint node in a TCP/IP packet-switched network, an ICMP
4 packet that includes a copy of a TCP header associated with a TCP
5 connection;
6 obtaining a packet sequence number from the TCP header;
7 determining if the packet sequence number is valid;
8 updating a maximum transmission unit (MTU) value associated with the TCP
9 connection only if the packet sequence number is determined to be valid.

1 11. A method as recited in Claim 10, wherein the step of receiving an ICMP packet
2 comprises receiving an ICMP “endpoint unreachable” error packet.

1 12. A method as recited in Claim 10, wherein the step of receiving an ICMP packet
2 comprises receiving an ICMP packet that specifies that fragmentation is needed.

1 13. A method as recited in Claim 10, wherein the step of determining if the packet
2 sequence number is valid comprises determining if the packet sequence number is within a
3 range of TCP packet sequence numbers that are allowed for the connection.

1 14. A method as recited in Claim 10, wherein the step of determining if the packet
2 sequence value is valid comprises determining if the packet sequence number is within a
3 range of sent but unacknowledged TCP packet sequence values for the connection.

1 15. A method as recited in Claim 10, wherein the step of determining if the packet
2 sequence value is valid comprises determining if the packet sequence number is equal to one
3 or more sequence numbers of one or more packets that are then-currently stored in a TCP re-
4 transmission buffer, starting at a sequence value of a previously sent segment that resulted in
5 receiving the ICMP packet.

1 16. A method as recited in Claim 10, wherein the steps are performed in a router acting as
2 a TCP endpoint node.

1 17. A method as recited in Claim 10, wherein the steps are performed in a firewall
2 device.

1 18. A computer-readable medium carrying one or more sequences of instructions, which
2 instructions, when executed by one or more processors, cause the one or more processors to
3 carry out the steps of any of claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, or 17.

1 19. Apparatus for preventing an attack on a network, comprising:
2 means for receiving an ICMP packet that includes a copy of a header associated with
3 a connection in a connection-oriented transport protocol;
4 means for obtaining a packet sequence value from the header;
5 means for determining if the packet sequence value is valid;

6 means for updating a parameter value associated with the transport protocol
7 connection only if the packet sequence value is determined to be valid.

1 20. An apparatus as recited in Claim 19, wherein the means for receiving an ICMP packet
2 comprises means for receiving an ICMP packet that includes a copy of a TCP header
3 associated with a TCP connection.

1 21. An apparatus as recited in Claim 19, wherein the means for receiving an ICMP packet
2 comprises means for receiving an ICMP “endpoint unreachable” error packet.

1 22. An apparatus as recited in Claim 19, wherein the means for receiving an ICMP packet
2 comprises means for receiving an ICMP packet that specifies that fragmentation is needed.

1 23. An apparatus as recited in Claim 19, wherein the means for determining if the packet
2 sequence value is valid comprises means for determining if the packet sequence value is
3 within a range of packet sequence values that are allowed by the transport protocol for the
4 connection.

1 24. An apparatus as recited in Claim 19, wherein the means for determining if the packet
2 sequence value is valid comprises means for determining if the packet sequence value is
3 within a range of sent but unacknowledged TCP packet sequence values for the connection.

1 25. An apparatus as recited in Claim 19, wherein the means for determining if the packet
2 sequence value is valid comprises means for determining if the packet sequence value is
3 equal to one or more sequence values of one or more packets that are then-currently stored in
4 a TCP re-transmission buffer.

1 26. An apparatus as recited in Claim 19, comprising a router acting as a TCP endpoint
2 node.

1 27. An apparatus as recited in Claim 19, comprising a firewall device.

1 28. A network element, comprising:

2 a network interface that is coupled to a data network for receiving one or more packet flows

3 therefrom;

4 a processor;

5 one or more stored sequences of instructions which, when executed by the processor, cause

6 the processor to carry out the steps of any of claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12,

7 13, 14, 15, 16, or 17.